Podróże po Imperium Liczb

Część 04. Liczby Pierwsze

Rozdział 6

6. Liczby pierwsze w postępach arytmetycznych

Andrzej Nowicki 22 stycznia 2013, http://www.mat.uni.torun.pl/~anow

Spis treści

Wszystkie książki z serii "Podróże po Imperium Liczb" napisano w edytorze LaTeX. Spisy treści tych książek oraz pewne wybrane rozdziały moża znaleźć na internetowej stronie autora: http://www-users.mat.uni.torun.pl/~anow.

6 Liczby pierwsze w postępach arytmetycznych

6.1 Twierdzenie Dirichleta

Peter Gustav Lejeune **Dirichlet** (1805 − 1859), niemiecki matematyk francuskiego pochodzenia. W 1837 roku Dirichlet udowodnił następujące twierdzenie, które dzisiaj nazywamy *twierdzeniem Dirichleta o liczbach pierwszych w postępie arytmetycznym.*

6.1.1 (Dirichlet, 1837)**.** *Jeśli a i b są względnie pierwszymi liczbami naturalnymi, to w ciągu*

$$a,\ a+b,\ a+2b,\ a+3b,\ a+4b,\ \ldots$$

istnieje nieskończenie wiele liczb pierwszych.

Wszystkie znane dowody tego twierdzenia są długie i nie są łatwe. Korzysta się w nich z różnych zaawansowanych twierdzeń. W polskiej literaturze matematycznej dowód twierdzenia Dirichleta znajdziemy w książkach Władysława Narkiewicza: [Nar77], [Nar03]. Poniżej podajemy pewną literaturę, w której są dowody tego twierdzenia lub dodatkowe informacje o tych dowodach. Znane są przeróżne dowody szczególnych przypadków twierdzenia Dirichleta. Takimi dowodami zajmować się będziemy w następnym rozdziale tej książki.

Omawiane twierdzenie Dirichleta ma liczne zastosowania. Pewne takie zastosowania przedstawiliśmy już w poprzednich rozdziałach. W innych książkach z serii "Podróże po Imperium Liczb" również znajdziemy zastosowania tego twierdzenia.

★ A. I. Gałoczkin, Y. V. Nesterenko, A. B. Szydłowski, *Twierdzenie Dirichleta o liczbach pierwszych w postępach arytmetycznych*, [G-ns] 59-93.

A. Granville, *On elementary proofs of the Prime Number Theorem for arithmetic progressions, without characters*, preprint.

E. Landau, *Dirichlet's theorem on the prime numbers in an arithmetic...*, [Land] 104-125.

P. Monsky, *Simplifying the proof of Dirichlet's theorem*, [Mon] 100(9)(1993) 861-862.

M. M. Postnikov, *Twierdzenie Dirichleta o liczbach pierwszych w postępach arytmetycznych*, dowód twierdzenia Dirichleta, dodatek w [Po82] 220-239.

A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, [AnnM] 50(1949) 297-304.

W. Sierpiński, *O pewnym tw. równoważnym tw. o postępie arytmetycznym*, [Wm] 7-29.

E. Trost, *Elementarny dowód twierdzenia o postępie arytmetycznym*, [Trost] 88-94.

6.2 Liczby pierwsze postaci ak + b

6.2.1. *Liczba postaci $2k-1$ jest pierwsza wtedy i tylko wtedy, gdy k nie jest postaci $2ab+a-b$, gdzie $a, b \in \mathbb{N}$, $a > 1$.* ([Mat] 5/52 62).

6.2.2. *Każda liczba pierwsza postaci $3k+1$ jest postaci $a^2 - ab + b^2$, gdzie $a, b \in \mathbb{N}$.*
([IrR] [B-ew] 147).

6.2.3 (K. Brown)**.** *Każda liczba pierwsza postaci* $3k+1$*:*

(1) *dzieli pewną liczbę postaci* a^2+3b^2*, gdzie* $(a,b)=1$*;*

(2) *dzieli pewną liczbę postaci* u^2+uv+v^2*, gdzie* $(u,v)=1$*;*

(3) *ma dokładnie jedno przedstawienie w postaci* a^2+3b^2*, gdzie* $(a,b)=1$*.*

6.2.4. *Tabela przedstawia liczby liczb pierwszych pewnych postaci* $ak+b$*, mniejszych od danej liczby naturalnej* n*.*

$n=$	100	500	1000	5000	10 000	100 000	500 000	1000 000
$3k+1$	11	45	80	330	611	4 784	20 733	39 231
$3k+2$	13	49	87	338	617	4 807	20 804	39 266
$4k+1$	11	44	80	329	609	4 783	20 731	39 175
$4k+3$	13	50	87	339	619	4 808	20 806	39 322
$5k+1$	5	22	40	163	306	2 387	10 386	19 617
$5k+2$	7	25	47	170	309	2 412	10 404	19 622
$5k+3$	7	24	42	172	310	2 402	10 382	19 665
$5k+4$	5	23	38	163	303	2 390	10 365	19 593
$6k+1$	11	45	80	330	611	4 784	20 733	39 231
$6k+5$	12	48	86	337	616	4 806	20 803	39 265

6.2.5. *Jeśli* p *jest liczbą pierwszą postaci* $3k+1$*, to równanie* $x^2+3y^2=4p$ *ma trzy różne rozwiązania naturalne.* ([B-ew] 147)*.*

6.2.6. *Niech* $p>2$ *będzie liczbą pierwszą postaci* $3k+2$ *i niech*

$$S=\{y^2-x^3-1;\ x,y\in\mathbb{Z},\ 0<x,y<p-1\}.$$

Wykazać, że w zbiorze S *jest co najmniej* $p-1$ *liczb podzielnych przez* p*.* ([Balk] 1999)*.*

6.2.7 (Fermat)**.** *Każda liczba pierwsza postaci* $4k+1$ *jest postaci* a^2+b^2*, gdzie* $a,b\in\mathbb{N}$ (*przedstawienie jest jednoznaczne*)*.*

6.2.8. *Każda liczba pierwsza dzieląca liczbę postaci* $4n^2+1$ *jest postaci* $4k+1$*.* ([Mon] 7(1983))*.*

6.2.9. *Dla każdej trójki* $(a,b,c)\in\mathbb{Z}^3$ *takiej, że* $ab\neq 0$*, istnieje* $n\in\mathbb{N}$ *takie, że liczba* an^2+bn+c *dzieli się przez liczbę pierwszą postaci* $4k+1$*.* ([Mon] 7(1983) E 2883)*.*

6.2.10. *Liczba postaci* $4k-1$ *jest pierwsza wtedy i tylko wtedy, gdy* k *nie jest postaci* $4ab+a-b$*, gdzie* $a,b\in\mathbb{N}$*.* ([Mat] 5/52 62, [S59] 360)*.*

D. Jeśli $k=4ab+a-b$, gdzie $a,b\in\mathbb{N}$, to $4k-1=16ab+4a-4b-1=(4a-1)(4b+1)$, a zatem $4k-1$ nie jest liczbą pierwszą.

Załóżmy teraz, że liczba k nie jest postaci $4ab+a-b$ ($a,b\in\mathbb{N}$) i przypuśćmy, że liczba $4k-1$ nie jest pierwsza. Istnieje wtedy liczba pierwsza, postaci $4a-1$, dzieląca $4k-1$. Niech $4k-1=(4a-1)u$, gdzie $u\in\mathbb{N}$. Wtedy liczba u musi być postaci $4b+1$, gdzie $b\in\mathbb{N}$. Mamy zatem: $4k-1=(4a-1)(4b+1)=16ab+4a-4b-1$, czyli $4k=16ab+4a-4b$, tzn. $k=4ab+a-b$, wbrew założeniu. ⊠

6.2.11. (1) *Każdą liczbę pierwszą postaci* $6n+1$ *można przedstawić w postaci* $\frac{1}{4}(a^2+27b^2)$, *gdzie* $a, b \in \mathbb{N}$.

(2) *Każdą liczbę pierwszą postaci* $6n+1$ *można przedstawić w postaci* x^2+xy+y^2, *gdzie* $x, y \in \mathbb{Z}$. ([Nagl] 265 z.123).

6.2.12. (1) *Liczba* $6n+1$ *jest pierwsza wtedy i tylko wtedy, gdy jedna z liczb postaci* $\frac{3n-r}{2r+1}$, *dla* $r = 1, 2, \ldots, n-1$, *jest całkowita.*

(2) *Liczba* $6n-1$ *jest pierwsza wtedy i tylko wtedy, gdy jedna z liczb postaci* $\frac{3n-r}{2r-1}$, *dla* $r = 2, 3 \ldots, n$, *jest całkowita.* ([Mon] NT-204).

6.2.13. *Liczba* $6n-1$ *jest pierwsza wtedy i tylko wtedy, gdy wśród liczb* $\frac{n-k}{6k-1}$, *gdzie* $k \in \mathbb{N}$, $k \neq n$, *nie ma ani jednej liczby całkowitej.* ([Mat] 1-2/63 76).

6.2.14 (H. Mroczkowska)**.** *Liczba postaci* $6n-1$ *jest pierwsza wtedy i tylko wtedy, gdy* n *nie jest postaci* $6ab+a-b$, *gdzie* $a, b \in \mathbb{N}$. ([Mat] 5/52 58, [S59] 360).

D. Jeśli $k = 6ab+a-b$, gdzie $a, b \in \mathbb{N}$, to $6k-1 = 36ab+6a-6b-1 = (6a-1)(6b+1)$, a zatem $6k-1$ nie jest liczbą pierwszą.

Załóżmy teraz, że liczba k nie jest postaci $6ab+a-b$ ($a, b \in \mathbb{N}$) i przypuśćmy, że liczba $6k-1$ nie jest pierwsza. Istnieje wtedy liczba pierwsza, postaci $6a-1$, dzieląca $6k-1$. Niech $6k-1 = (6a-1)u$, gdzie $u \in \mathbb{N}$. Wtedy liczba u musi być postaci $6b+1$, gdzie $b \in \mathbb{N}$. Mamy zatem: $6k-1 = (6a-1)(6b+1) = 36ab+6a-6b-1$, czyli $6k = 36ab+6a-6b$, tzn. $k = 6ab+a-b$, wbrew założeniu. ☒

6.2.15 ([Mon] 79(6)(1972) s.761)**.**

(1) *Każda liczba pierwsza postaci* $8k+1$ *daje się przedstawić w postaci* x^2-2y^2, *gdzie* x, y *są liczbami całkowitymi.*

(2) *Z równości* $x^2-2y^2 = (3x+4y)^2-2(2x+3y)^2$ *wynika, że rozkładów, o których mowa w* (1), *istnieje nieskończenie wiele.*

6.2.16. *Liczba pierwsza* p *jest postaci* $8n \pm 1$ *wtedy i tylko wtedy, gdy istnieje liczba całkowita* k *taka, że* $p^2 = 48k+1$. ([Ama] F-1).

6.2.17. *Niech* p *będzie liczbą pierwszą postaci* $8k \pm 3$ *i niech* $a, b \in \mathbb{Z}$. *Jeśli* $p \mid a^2-2b^2$, *to* $p \mid a$ *i* $p \mid b$. ([Miss] 1997 z.107).

6.2.18. *Każdą liczbę pierwszą postaci* $11n+r$, *gdzie* $r \in \{1, 3, 4, 5, 9\}$ *można przedstawić w postaci* $x^2+xy+3y^2$, *gdzie* $x, y \in \mathbb{Z}$. *Wszystkie pozostałe liczby pierwsze, różne od* 11, *nie mają tej własności.* ([Nagl] 266 z.126).

6.2.19 (A. Wakulicz)**.** *Liczba postaci* $12k+5$ *jest pierwsza wtedy i tylko wtedy, gdy* k *nie jest postaci* $5x+(12x+1)y$, *gdzie* $x, y \in \mathbb{Z}$. ([S59] 346).

6.2.20. *Każdą liczbę pierwszą postaci* $24n+1$ *lub* $24k+7$ *można przedstawić w postaci* a^2+6b^2, *gdzie* $a, b \in \mathbb{N}$. *Wszystkie pozostałe liczby pierwsze nie mają tej własności.* ([Nagl] 266 z.124).

6.2.21. *Każdą liczbę pierwszą postaci* $24n+1$ *lub* $24k+19$ *można przedstawić w postaci* $3a^2-2b^2$, *gdzie* $a, b \in \mathbb{N}$. *Wszystkie pozostałe liczby pierwsze nie mają tej własności.* ([Nagl] 267 z.132).

6.2.22. *Każdą liczbę pierwszą postaci* $24n + 5$ *lub* $24k + 23$ *można przedstawić w postaci* $2a^2 - 3b^2$, *gdzie* $a, b \in \mathbb{N}$. *Wszystkie pozostałe liczby pierwsze nie mają tej własności.* ([Nagl] 267 z.132).

6.2.23. *Każdą liczbę pierwszą postaci* $40n + r$, *gdzie* $r \in \{7, 13, 23, 37\}$ *można przedstawić w postaci* $2a^2 + 5b^2$, *gdzie* $a, b \in \mathbb{N}$. *Wszystkie pozostałe liczby pierwsze nie mają tej własności.* ([Nagl] 266 z.125).

6.2.24. *Niech* $a, b \in \mathbb{N}$, $(a, b) = 1$. *Każda liczba naturalna postaci* $ak+b$ *ma dzielnik pierwszy postaci* $ak+b$ *wtedy i tylko wtedy, gdy para* (a, b) *należy do zbioru* $\{(2, 1),\ (3, 2),\ (4, 3),\ (6, 5)\}$. ([Mat] 5/52 63).

★ J. T. B. Beard, Jr., *Are all primes* $32k + 17$ *square separable?*, [Mon] 87(9)(1980) 744-745.

Monika Hagedorn, *Graficzne interpretacje rozmieszczenia liczb pierwszych w ciągu liczb naturalnych*, [Pmgr] 1999.

J. W. Matijasewicz, *Formuły dla liczb pierwszych* (również o dywanach Ulama), [Kw] 5/75 5-13.

Mariusz Olesiak, *Rozmieszczenie liczb pierwszych. Spirale Ulama*, [Pmgr] 2011.

A. M. Vaidya, *On primes in a.p.*, [MM] 40(1)(1967) 29-30.

A. P. Winniczenko, *O dywanach Ulama*, [Kw] 4/75 21-26.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

6.3 Skończone ciągi kolejnych liczb naturalnych i liczby pierwsze

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

6.3.1. *Dla dowolnej liczby naturalnej* n *istnieje* n *kolejnych liczb naturalnych złożonych.*

D. Niech $a = (n + 1)! + 1$. Wtedy wszystkie liczby $a + 1, a + 2, \ldots, a + n$ są złożone. ⊠

6.3.2 (Maple)**.** *Najdłuższe ciągi kolejnych liczb naturalnych złożonych, mniejszych od danej liczby naturalnej* n. *Długość ciągu oznaczono przez* d.

$$
\begin{aligned}
n = 100: &\quad (90, 91, \ldots, 96), && d = 7;\\
n = 200: &\quad (114, 115, \ldots, 126), && d = 13;\\
n = 600: &\quad (524, 525, \ldots, 540), && d = 17;\\
n = 1\,000: &\quad (888, 889, \ldots, 906), && d = 19;\\
n = 2\,000: &\quad (1328, 1329, \ldots, 1360), && d = 33;\\
n = 10\,000: &\quad (9552, 9553, \ldots, 9586), && d = 35;\\
n = 100\,000: &\quad (31398, 31399, \ldots, 31468), && d = 71;\\
n = 400\,000: &\quad (370262, 370263, \ldots, 370372), && d = 111;\\
n = 1\,000\,000: &\quad (492114, 492115, \ldots, 492226), && d = 113;\\
n = 10\,000\,000: &\quad (4652354, 4652355, \ldots, 4652506), && d = 153.
\end{aligned}
$$

W konkursie matematycznym "Turnament of the Town" z 2001 roku pojawiło się następujące pytanie.

6.3.3. *Czy istnieje* 1000 *kolejnych liczb naturalnych, wśród których jest dokładnie* 5 *liczb pierwszych?* ([TT] 2001).

O. Tak, istnieje! Wykazać to można w następujący sposób. Każdy ciąg składający się z 1000 kolejnych liczb naturalnych nazwijmy 1000-blokiem.

Napierw zauważamy, że istnieje taki 1000-blok, w którym nie ma żadnej liczby pierwszej (patrz 6.3.1). Spośród wszystkich takich 1000-bloków bez liczby pierwszej wybieramy blok najmniejszy, tzn. taki blok, który ma najmnieszą liczbę początkową. Oznaczmy przez n_0 liczbę początkową tego najmniejszego bloku.

Wszystkie liczby wystąpujące w tym wybranym bloku pomniejszamy o 1. Otrzymujemy w ten sposób 1000-blok z dokładnie jedną liczbą pierwszą. Istnieją więc 1000-bloki o takich wyrazach, wśród których jest dokładnie jedna liczba pierwsza. Spośród wszystkich takich bloków wybierzmy blok najmniejszy. Liczbę początkową tego wybranego bloku oznaczmy przez n_1. Oczywiście $n_1 < n_0$.

Wszystkie liczby wystąpujące w tym wybranym bloku pomniejszamy o 1. Otrzymujemy w ten sposób 1000-blok z dokładnie dwiema liczbami pierwszymi. To, że są tu dokładnie dwie liczby pierwsze wymaga wyjaśnienia. Jest oczywiste, że są tu co najwyżej dwie liczby pierwsze. Ponieważ $n_1 < n_0$, więc co najmniej jedna liczba pierwsza muśi być. Z nierówności $n_1 - 1 < n_1$ wynika, że nie może być dokładnie jedna liczba pierwsza. Są więc tu dokładnie dwie liczby pierwsze.

Spośród wszystkich 1000-bloków o dokładnie dwóch liczbach pierwszych wybieramy blok najmniejszy i powtarzamy powyższe rozumowanie. W ten spośb otrzymujemy kolejno 1000-bloki mające dokładnie odpowiednio 3, 4, 5, 6, ... liczb pierwszych. Ponieważ w najmniejszym 1000-bloku $(1, 2, 3, \ldots, 1000)$ jest więcej niż 5 liczb pierwszych, więc przy pomocy opisanej konstrukcji natrafimy na 1000-blok posiadający dokładnie 5 liczb pierwszych. ☒

W ten sam sposób uzasadniamy następujące stwierdzenia.

6.3.4. *Dla każdej liczby naturalnej n istnieje n kolejnych liczb naturalnych, wśród których jest dokładnie jedna liczba pierwsza.*

6.3.5. *Dla każdej liczby naturalnej $n \geqslant 3$ istnieje n kolejnych liczb naturalnych, wśród których są dokładnie dwie liczby pierwsze.*

6.3.6. *Istnieje* 100 *kolejnych liczb naturalnych, wśród których jest dokładnie* 10 *liczb pierwszych.*

U. Taką własność posiada ciąg $1298, 1299, \ldots, 1397$. Jest to najmniejszy ciąg tego rodzaju. ☒

6.3.7. *Istnieje* 1000 *kolejnych liczb naturalnych, wśród których jest dokładnie* 100 *liczb pierwszych.*

U. Taką własność posiada ciąg $10344, 10345, \ldots, 11343$. Jest to najmniejszy taki ciąg. ☒

6.3.8. *Jeśli $n > 8$ jest liczbą naturalną, to co najmniej jedna z liczb n i $n + 1$ ma dzielnik pierwszy większy od* 3. ([S59] 331).

6.3.9 (A.Mąkowski 1968)**.** *Liczby $m = 3 \cdot 5^2$ i $n = 3^5 \cdot 5$ mają identyczne dzielniki pierwsze. Tę samą własność mają liczby $m + 1 = 2^2 \cdot 19$ i $n + 1 = 2^6 \cdot 19$.* ([Gy04] 113).

6.3.10. *Niech $n \geqslant 4$. Liczby n i $n + 1$ są jednocześnie złożone wtedy i tylko wtedy, gdy najbliższa liczba całkowita liczby $\frac{(n-1)!}{n^2+n}$ jest parzysta.* ([Mon] 98(1)(1991) 60-62 E3308).

6.3.11. *Wśród trzech kolejnych liczb naturalnych > 7 istnieje co najmniej jedna, która ma dwa różne dzielniki pierwsze.* ([Mat] 3/62 190, [S64] 80).

6.3.12. *Wśród czterech kolejnych liczb naturalnych* > 24 *istnieje co najmniej jedna, która ma trzy parami różne dzielniki pierwsze.* ([S64] 80a).

6.3.13. *Istnieją trzy kolejne liczby naturalne będące iloczynami dwóch różnych liczb pierwszych. Przykłady:* $33, 34, 35$*;* $85, 86, 87$*;* $93, 94, 95$*;* $141, 142, 143$*;* $201, 202, 203$. ([S64] 81).

6.3.14. *Istnieją cztery kolejne liczby naturalne, z których każda ma dokładnie dwa różne dzielniki pierwsze. Np.* $33 = 3 \cdot 11$, $34 = 2 \cdot 17$, $35 = 5 \cdot 7$, $36 = 2^2 \cdot 3^2$. ([S64] 81).

6.3.15. *Dla każdych* 6 *kolejnych liczb naturalnych istnieje liczba pierwsza, która dzieli tylko jedną z tych sześciu liczb.* ([OM] Niemcy 2002/2003).

6.3.16. *Zbioru* $\{n, n+1, n+2, n+3, n+4, n+5\}$ *nie można podzielić na dwa rozłączne podzbiory tak, by iloczyny liczb występujących w tych podzbiorach były jednakowe.*
([Kw] 2/71 55,62).

6.3.17. *Wśród* 10 *kolejnych liczb naturalnych:*

(1) *istnieje taka liczba, która jest względnie pierwsza z każdą z pozostałych liczb;*
([S50] 7, [Br83] 8).

(2) *znajduje się zawsze co najmniej jedna, a co najwyżej cztery liczby niepodzielne przez* 2, 3, 5 *i* 7*;* ([S59] 360, [Str] 14).

(3) *są co najwyżej* 4 *nieparzyste liczby pierwsze.* ([S59] 360).

6.3.18. *Wśród* 12 *kolejnych liczb naturalnych większych niż* 3 *jest co najmniej* 8 *liczb złożonych.* ([S50] 26).

6.3.19. *W ciągu* $a+1,\ a+2,\ \ldots,\ a+14$*, gdzie* $a \in \mathbb{Z}$*, istnieje liczba, która nie jest podzielna przez* $2, 3, 5, 7, 11$. ([S59] 361).

6.3.20. *Znaleźć co najmniej jedną liczbę naturalną* n *taką, że każda z liczb* $n, n+1, n+2, \ldots, n+20$ *ma wspólny czynnik większy od* 1 *z liczbą* $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. Odp. *Np.* $n = 9440$*, jest to najmniejsze takie* n. ([OM] ZSRR 1981, [WaJ] 322(80)).

6.3.21. *W ciągu* $a+1,\ a+2,\ \ldots,\ a+22$*, gdzie* $a \in \mathbb{Z}$*, istnieje liczba, która nie jest podzielna przez* $2, 3, 5, 7, 11, 13$. ([S59] 361).

6.3.22. *W ciągu* $a+1,\ a+2,\ \ldots,\ a+26$*, gdzie* $a \in \mathbb{Z}$*, istnieje liczba, która nie jest podzielna przez* $2, 3, 5, 7, 11, 13, 17$. ([S59] 361).

6.3.23. *W ciągu* $n+1,\ n+2,\ \ldots,\ n+100$*, gdzie* $n > 1$*, istnieje co najwyżej* 25 *liczb pierwszych.* ([S59] 363).

6.3.24. *W ciągu* $n+1,\ n+2,\ \ldots,\ n+100$ *są zawsze co najmniej trzy takie liczby, które są podzielne przez* 7 *i nie są podzielne przez* $2, 3$ *oraz* 5. ([Mat] 4/56 69).

6.3.25. *Niech $m_1, m_2, \ldots, m_s$ będą parami względnie pierwszymi liczbami naturalnymi. Istnieje wtedy nieskończenie wiele liczb naturalnych a takich, że wszystkie liczby*

$$a+1,\ a+2,\ \ldots,\ a+n$$

są złożone oraz $m_i \mid a+i$ dla $i = 1, 2, \ldots, n$. (Grimm 1955).

D. Wynika to na przykład z twierdzenia chińskiego o resztach. Mamy parami względnie pierwsze liczby $m_1^2, m_2^2, \ldots, m_n^2$ i na mocy twierdzenia chińskiego o resztach istnieje niskończenie wiele liczb naturalnych a takich, że $a \equiv -i \pmod{m_i^2}$ dla $i = 1, 2, \ldots, n$. ⊠

6.3.26. *Dla każdej liczby naturalnej $n > 1$ istnieje $2p_{n-1} - 1$ kolejnych liczb naturalnych, z których każda ma dzielnik pierwszy nie większy niż $\leqslant p_n$.* ([S59] 362).

6.3.27. *Niech $a+1, a+2, \ldots, a+n$ będą kolejnymi liczbami naturalnymi przy czym $a > n^{n-1}$. Istnieje wtedy n parami różnych liczb pierwszych $p_1, \ldots, p_n$ takich, że $p_i \mid a+i$ dla $i = 1, 2, \ldots, n$.* (Grimm 1961).

6.3.28. *Jeśli liczby naturalne k i n spełniają nierówność $k > n!$, to istnieją parami różne liczby pierwsze $p_1, p_2, \ldots, p_n$ będące odpowiednio dzielnikami liczb $k+1, k+2, \ldots, k+n$.* ([OM] Polska 2010).

D. ([OMs]). Dla $i = 1, 2, \ldots, n$ niech a_i oznacza najmniejszą wspólną wielokrotność tych dzielników liczby $k+i$, które nie przekraczają n.

Najmniejsza wspólna wielokrotność liczb nie przekraczających n jest nie większa niż $n!$, więc (ponieważ $k > n!$)

$$a_i < k \quad \text{dla} \quad i = 1, 2, \ldots, n. \tag{1}$$

Z drugiej strony, dla każdego $i = 1, 2, \ldots, n$ liczba a_i jest najmniejszą wspólną wielokrotnością dzielników liczby $k+i$. Wobec tego sama jest dzielnikiem liczby $k+i$. Liczby

$$\tfrac{k+1}{a_1},\ \tfrac{k+2}{a_2},\ \ldots,\ \tfrac{k+n}{a_n} \tag{2}$$

są zatem całkowite, a nierówności (1) wskazują, że są one większe od 1.

Wykażemy, że liczby (2) są parami względnie pierwsze. W tym celu rozpatrzmy różne wskaźniki $i, j \in \{1, 2, \ldots, \}$. Liczby $k+i$ oraz $k+j$ różnią się o mniej niż n, więc ich największy wspólny dzielnik $d = \operatorname{nwd}(k+i, k+j)$ nie przekracza n i wobec tego jest dzielnikiem liczb a_i i a_j. To oznacza, że liczby $\frac{k+i}{a_i}$ oraz $\frac{k+j}{a_j}$ są odpowiednio dzielnikami liczb $\frac{k+i}{d}$ oraz $\frac{k+j}{d}$. Te ostatnie są oczywiście względnie pierwsze.

W efekcie liczby (2) są parami względnie pierwszymi liczbami większymi od 1. Są one jednak odpowiednio dzielnikami liczb $k+1, k+2, \ldots, k+n$. Teza będzie więc spełniona, jeżeli za $p_1, p_2, \ldots, p_n$ przyjmiemy dowolne dzielniki pierwsze odpowiednio liczb (2). ⊠

6.3.29 (Hipoteza, Grimm 1969)**.** *Jeśli wszystkie liczby $a+1, a+2, \ldots, a+n$ są złożone, to istnieją parami różne liczby pierwsze $p_1, p_2, \ldots, p_m$ takie, że $p_1 \mid a+1$, $p_2 \mid a+2, \ldots,$ $p_n \mid a+n$.* ([Gy04] 133).

6.3.30 ([Gy04] 133)**.** *Przykłady potwierdzające hipotezę* 6.3.29.

(1)

1802	1803	1804	1805	1806	1807	1808	1809	1810
53	601	41	19	43	139	113	67	181.

(2)

114	115	116	117	118	119	120	121	122	123	124	125	126
19	23	29	13	59	17	2	11	61	41	31	5	7.

([Gy04] 133).

6.3.31 (Erdös)**.** *Niech $n, k \in \mathbb{N}$, $n \geqslant k$. Istnieje wtedy liczba pierwsza $p \geqslant k+1$ dzieląca jedną z liczb $n+1, n+2, \ldots, n+k$.* ([Fila] 33).

6.3.32. *W skończonym ciągu $n, n+1, n+2, \ldots, n+k$ istnieje zawsze liczba podzielna przez pewną taką potęgę liczby 2, przez którą nie jest podzielna żadna inna liczba tego ciągu.* ([S50] 12).

6.3.33. *Dla każdej liczby naturalnej k istnieje liczba naturalna n taka, że wśród liczb $n+1, n+2, \ldots, n+k$ nie ma żadnej potęgi liczby pierwszej.* ([IMO]).

6.3.34. *Znaleźć wszystkie piątki kolejnych liczb naturalnych nieparzystych, z których każda jest potęgą liczby pierwszej o wykładniku naturalnym.* ([Mat] 5/2001 z.1517).

O. Są tylko trzy takie piątki: $(3,5,7,9,11)$, $(5,7,9,11,13)$ i $(23,25,27,29,31)$. Jedyną szóstką o rozpatrywanej własności jest $(3,5,7,9,11,13)$. Siódemek takich nie ma. ☒

★ E. F.Ecklund, R. B. Eggleton, *Prime factors of consecutive...*, [Mon] 79(10)(1972) 1082-1089.
E. F.Ecklund, R. B. Eggleton, *A note on consecutive composite...*, [MM] 48(5)(1975) 277-281.
C. A. Grimm, *A note on consecutive composite numbers*, [Mon] 68(1961) 781.
C. A. Grimm, *A conjecture on consecutive composite numbers*, [Mon] 76(1969) 1126-1128.
R. K. Guy, *Grimm's conjecture*, [Gy04] 133-134.
B. Leszczyński, *Pewna hipoteza o podzielnikach pierwszych kolejnych liczb nat.*, [Mat] 1/66 3-4.

6.4 Kolejne wyrazy skończonych ciągów arytmetycznych

6.4.1. *W każdym rosnącym ciągu arytmetycznym o wyrazach naturalnych istnieją dowolnie długie skończone ciągi jego kolejnych wyrazów, z których każdy jest liczbą złożoną.* ([Mon] 25(4)(1918) 179-180, [S64] 53).

D. Niech a i b będą liczbami naturalnymi i niech $x_n = a+nb$ dla $n = 1, 2, \cdots$. Niech k będzie liczbą naturalną. Wykażemy, że istnieje $n \in \mathbb{N}$ takie, że wszystkie liczby $x_{n+1}, x_{n+2}, \ldots, x_{n+k}$ są liczbami złożonymi.

Rozpatrzmy liczby naturalne $x_1, x_2, \ldots, x_k$. Wszystkie one są większe od 1. Niech $n = x_1 x_2 \cdots x_k$. Wtedy dla każdego i należącego do zbioru $\{1, 2, \ldots, k\}$ zachodzą równości

$$x_{n+i} = a + (n+i)b = (a+ib) + nb = x_i + x_1 \cdots x_i \cdots x_k b.$$

Każda więc liczba x_{n+i} (dla $i = 1, 2, \ldots, k$) jest większa od x_i i jest podzielna przez większą od jedynki liczbę x_i; jest więc liczbą złożoną. ☒

6.4.2. *Czy istnieje* 1000 *kolejnych liczb naturalnych postaci $4k+1$, wśród których jest dokładnie* 5 *liczb pierwszych?*

O. Tak, istnieje! Wykazać to można w następujący sposób, podobny do tego sposobu zastosowanego w 6.3.3. Każdy ciąg składający się z 1000 kolejnych liczb naturalnych postaci $4k+1$ nazwijmy 1000-blokiem.

Najpierw zauważamy, że istnieje taki 1000-blok, w którym nie ma żadnej liczby pierwszej (patrz 6.4.1). Spośród wszystkich takich 1000-bloków bez liczby pierwszej wybieramy blok najmniejszy, tzn. taki blok, który ma najmnieszą liczbę początkową. Oznaczmy przez n_0 liczbę początkową tego najmniejszego bloku.

Wszystkie liczby wystąpujące w tym wybranym bloku pomniejszamy o 4. Otrzymujemy w ten sposób 1000-blok z dokładnie jedną liczbą pierwszą. Istnieją więc 1000-bloki o takich wyrazach, wśród których jest dokładnie jedna liczba pierwsza. Spośród wszystkich takich bloków wybierzmy blok najmniejszy. Liczbę początkową tego wybranego bloku oznaczmy przez n_1. Oczywiście $n_1 < n_0$.

Wszystkie liczby wystąpujące w tym wybranym bloku pomniejszamy o 4. Otrzymujemy w ten sposób 1000-blok z dokładnie dwiema liczbami pierwszymi. To, że są tu dokładnie dwie liczby pierwsze wymaga wyjaśnienia. Jest oczywiste, że są tu co najwyżej dwie liczby pierwsze. Ponieważ $n_1 < n_0$, więc co najmniej jedna liczba pierwsza musi być. Z nierówności $n_1 - 1 < n_1$ wynika, że nie może być dokładnie jedna liczba pierwsza. Są więc tu dokładnie dwie liczby pierwsze.

Spośród wszystkich 1000-bloków o dokładnie dwóch liczbach pierwszych wybieramy blok najmniejszy i powtarzamy powyższe rozumowanie. W ten spośb otrzymujemy kolejno 1000-bloki posiadające dokładnie odpowiednio 3, 4, 5, 6,... liczb pierwszych. Ponieważ w najmniejszym 1000-bloku $(1, 5, 9, \ldots, 3997)$ jest więcej niż 5 liczb pierwszych (patrz tablica 6.2.4), więc przy pomocy opisanej konstrukcji natrafimy na 1000-blok posiadający dokładnie 5 liczb pierwszych. ⊠

W ten sam sposób uzasadniamy następujące stwierdzenia.

6.4.3. *Niech a, b będą względnie pierwszymi liczbami naturalnymi. Dla każdej liczby naturalnej n istnieje n kolejnych liczb naturalnych postaci $ak + b$, wśród których jest dokładnie jedna liczba pierwsza.*

D. Każdy ciąg składający się z n kolejnych liczb naturalnych postaci $ak + b$ nazwijmy blokiem. Wiemy (na mocy twierdzenia Dirichleta), że istnieje co najmniej jedna liczba pierwsza p postaci $ak+b$.

Poprawiając nieco dowód faktu 6.4.1 stwierdzamy najpierw, że istnieje taki blok o wyrazach większych od p, w którym nie ma żadnej liczby pierwszej. Spośród wszystkich takich bloków bez liczby pierwszej wybieramy blok najmniejszy, tzn. taki blok, który ma najmnieszą liczbę początkową. Wszystkie liczby wystąpujące w tym wybranym bloku pomniejszamy o a i otrzymujemy blok spełniający tezę. ⊠

6.4.4. *Istnieje* 100 *kolejnych liczb naturalnych postaci $4k + 3$, wśród których jest dokładnie* 10 *liczb pierwszych.*

6.4.5. *Istnieje* 1000 *kolejnych liczb naturalnych postaci $6k + 1$, wśród których jest dokładnie* 50 *liczb pierwszych.*

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

6.5 Skończone postępy arytmetyczne liczb pierwszych

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Każde dwie liczby pierwsze tworzą oczywiście skończony (dwuelementowy) ciąg arytmetyczny. Liczby pierwsze $3, 5, 7$ tworzą ciąg arytmetyczny o długości 3. Taki ciąg tworzą też liczby pierwsze $3, 7, 11$.

6.5.1. *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 3 (*r oznacza stałą różnicę*).

r	*ciąg*
2	$(3, 5, 7)$
4	$(3, 7, 11)$
8	$(3, 11, 19)$
10	$(3, 13, 23)$
14	$(3, 17, 31)$
20	$(3, 23, 43)$
28	$(3, 31, 59)$
34	$(3, 37, 71)$

r	*ciąg*
38	$(3, 41, 79)$
40	$(3, 43, 83)$
50	$(3, 53, 103)$
64	$(3, 67, 131)$
68	$(3, 71, 139)$
80	$(3, 83, 163)$
94	$(3, 97, 191)$
98	$(3, 101, 199)$

r	*ciąg*
104	$(3, 107, 211)$
110	$(3, 113, 223)$
124	$(3, 127, 251)$
134	$(3, 137, 271)$
154	$(3, 157, 311)$
164	$(3, 167, 331)$
178	$(3, 181, 359)$
188	$(3, 191, 379)$

W powższych przykładach każdy postęp rozpoczyna się liczbą 3.

6.5.2. *Jeśli trzy liczby pierwsze tworzą postęp arytmetyczny o różnicy niepodzielnej przez* 6*, to najmniejszą z tych liczb jest* 3. ([Str67] 10, [B-rs] 174, patrz 6.5.26 i 6.5.28).

6.5.3. *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 3 *o różnicy* r *podzielnej przez* 6.

r	*ciąg*
6	$(7, 13, 19)$
6	$(17, 23, 29)$
6	$(31, 37, 43)$
6	$(47, 53, 59)$
6	$(67, 73, 79)$
6	$(97, 103, 109)$
6	$(101, 107, 113)$
6	$(151, 157, 163)$
6	$(167, 173, 179)$

r	*ciąg*
12	$(19, 31, 43)$
12	$(29, 41, 53)$
12	$(59, 71, 83)$
12	$(89, 101, 113)$
12	$(139, 151, 163)$
12	$(167, 179, 191)$
12	$(199, 211, 223)$

r	*ciąg*
18	$(11, 29, 47)$
18	$(23, 41, 59)$
18	$(61, 79, 97)$
18	$(71, 89, 107)$
18	$(131, 149, 167)$
18	$(163, 181, 199)$
18	$(193, 211, 229)$

r	*ciąg*
24	$(5, 29, 53)$
24	$(13, 37, 61)$
24	$(19, 43, 67)$
24	$(23, 47, 71)$
24	$(83, 107, 131)$
24	$(89, 113, 137)$
24	$(103, 127, 151)$
24	$(149, 173, 197)$

6.5.4.

(1) *Jedynym* 3*-wyrazowym ciągiem arytmetycznym liczb pierwszych o różnicy* 8 *jest ciąg* $(3, 11, 19)$. ([Mat] 3/59 135, [S59] 350).

(2) *Jedynym* 3*-wyrazowym ciągiem arytmetycznym liczb pierwszych o różnicy* 10 *jest ciąg* $(3, 13, 23)$. ([S59] 350, [S64] 62).

(3) *Nie ma żdanego* 3*-wyrazowego ciągu arytmetycznego liczb pierwszych o różnicy* 100. ([Mat] 2/57 62, [S59] 351, [S64] 63).

(4) *Nie ma żdanego* 3*-wyrazowego ciągu arytmetycznego liczb pierwszych o różnicy* 1000. ([S64] s.56).

6.5.5 (van der Corput 1933, S.Chowla 1944)**.** *Istnieje nieskończenie wiele trójwyrazowych postępów arytmetycznych, utworzonych z różnych liczb pierwszych.* ([S59] 349, [Gr08]).

U. Jest to równoważne z tym, że równanie $p+q = 2r$ ma nieskończenie wiele rozwiązań w liczbach pierwszych p, q, r, gdzie $p \neq q$. ⊠

6.5.6 (A.Balog 1990)**.** *W poniższym* 3×3 *kwadracie*

11	17	23
59	53	47
107	89	71

są same liczby pierwsze. W każdym wierszu i w każdej kolumnie mamy ciąg arytmetyczny. Tego rodzaju 3×3 *kwadratów istnieje nieskończenie wiele,* ([Balo], [Gr08]).

6.5.7 (A.Balog 1990)**.** *Spójrzmy na* $3 \times 3 \times 3$ *liczbowy sześcian, którego pierwsze, drugie i trzecie piętro jest odpowiednio równe:*

47	483	2719
179	431	683
311	479	647

149	401	653
173	347	521
197	293	389

251	419	587
167	263	359
83	107	131

Wszystkie występujące tu liczby są pierwsze. W każdym wierszu i w każdej kolumnie mamy ciąg arytmetyczny. W każdym słupku pionowym również jest ciąg arytmetyczny. Tego rodzaju $3 \times 3 \times 3$ *sześcianów istnieje nieskończenie wiele,* ([Balo], [Gr08]).

6.5.8 (B.Green, T.Tao, 2005)**.** *Dla każdej liczby naturalnej n istnieje nieskończenie wiele n-wyrazowych postępów arytmetycznych utworzonych z parami różnych liczb pierwszych.* ([G-T]).

U. ([Gr08]). Praca [G-T] jest bazowana na ideach pochodzących z analizy harmonicznej, teorii ergodycznej, geometrii dyskretnej, addytywnej teorii liczb, kombinatoryki. Green i Tao potrafią udowodnić, że dla każdej liczby naturalnej n istnieje n-wyrazowy ciąg arytmetyczny zbudowany z liczb pierwszych mniejszych od liczby

$$2^{2^{2^{2^{2^{2^{2^{100n}}}}}}}.$$

Jest hipoteza, Granville z 2008 roku, że tę liczbą można zmniejszyć do liczby $n! + 1$. ☒

6.5.9. *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 4 (r *oznacza stałą różnicę*).

r	*ciąg*
6	$(11, 17, 23, 29)$
6	$(41, 47, 53, 59)$
6	$(61, 67, 73, 79)$
12	$(7, 19, 31, 43)$
12	$(17, 29, 41, 53)$
12	$(47, 59, 71, 83)$
12	$(127, 139, 151, 163)$
18	$(5, 23, 41, 59)$
18	$(43, 61, 79, 97)$
18	$(53, 71, 89, 107)$
18	$(113, 131, 149, 167)$
24	$(59, 83, 107, 131)$
24	$(79, 103, 127, 151)$

r	*ciąg*
30	$(13, 43, 73, 103)$
30	$(23, 53, 83, 113)$
30	$(41, 71, 101, 131)$
30	$(67, 97, 127, 157)$
30	$(167, 197, 227, 257)$
30	$(181, 211, 241, 271)$
36	$(31, 67, 103, 139)$
42	$(47, 89, 131, 173)$
42	$(67, 109, 151, 193)$
42	$(97, 139, 181, 223)$
42	$(107, 149, 191, 233)$
42	$(157, 199, 241, 283)$
48	$(13, 61, 109, 157)$

6.5.10. *W poniższym* 4×4 *kwadracie*

83	131	179	277
251	257	263	269
419	383	347	311
587	509	431	353

są same liczby pierwsze. W każdym wierszu i w każdej kolumnie mamy ciąg arytmetyczny. ([Gr08]).

6.5.11. *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 5 (r *oznacza stałą różnicę*).

r	*ciąg*
6	$(5, 11, 17, 23, 29)$
12	$(5, 17, 29, 41, 53)$
42	$(5, 47, 89, 131, 173)$
48	$(5, 53, 101, 149, 197)$
96	$(5, 101, 197, 293, 389)$
126	$(5, 131, 257, 383, 509)$

W powższych przykładach każdy postęp rozpoczyna się liczbą 5.

6.5.12. *Jeśli liczby pierwsze* $p_1 < p_2 < p_3 < p_4 < p_5$ *tworzą postęp arytmetyczny o różnicy niepodzielnej przez* 30*, to* $p_1 = 5$. (Patrz 6.5.26 i 6.5.28).

6.5.13. *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 5 *o różnicy* r *podzielnej przez* 30.

r	*ciąg*
30	$(11, 41, 71, 101, 131)$
30	$(37, 67, 97, 127, 157)$
30	$(137, 167, 197, 227, 257)$
30	$(151, 181, 211, 241, 271)$
60	$(43, 103, 163, 223, 283)$
60	$(71, 131, 191, 251, 311)$
60	$(113, 173, 233, 293, 353)$
90	$(61, 151, 241, 331, 421)$

r	*ciąg*
90	$(83, 173, 263, 353, 443)$
90	$(89, 179, 269, 359, 449)$
90	$(103, 193, 283, 373, 463)$
120	$(29, 149, 269, 389, 509)$
120	$(107, 227, 347, 467, 587)$
150	$(13, 163, 313, 463, 613)$
150	$(17, 167, 317, 467, 617)$
180	$(101, 281, 461, 641, 821)$

6.5.14.

(1) *Jedynym* 5*-wyrazowym ciągiem arytmetycznym liczb pierwszych o różnicy* 6 *jest ciąg* $(5, 11, 17, 23, 29)$. ([S59] 349).

(2) *Jedynym* 5*-wyrazowym ciągiem arytmetycznym liczb pierwszych o różnicy* 12 *jest ciąg* $(5, 17, 29, 41, 53)$. ([Mat] 3/59 135, [S59] 351).

(3) *Jedynym* 5*-wyrazowym ciągiem arytmetycznym liczb pierwszych o różnicy* 42 *jest ciąg* $(5, 47, 89, 131, 173)$. ([Mat] 3/59 135, [S59] 351).

6.5.15. *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 6 (r *oznacza stałą różnicę*).

r	*ciąg*
30	$(7, 37, 67, 97, 127, 157)$
30	$(107, 137, 167, 197, 227, 257)$
60	$(11, 71, 131, 191, 251, 311)$
60	$(53, 113, 173, 233, 293, 353)$
90	$(13, 103, 193, 283, 373, 463)$
150	$(73, 223, 373, 523, 673, 823)$
150	$(157, 307, 457, 607, 757, 907)$
210	$(13, 223, 433, 643, 853, 1063)$
240	$(23, 263, 503, 743, 983, 1223)$
300	$(83, 383, 683, 983, 1283, 1583)$
330	$(127, 457, 787, 1117, 1447, 1777)$

6.5.16. *Dwie szóstki liczb pierwszych tworzących postęp arytmetyczny o różnicy* 30*:*

$$541, 571, 601, 631, 661, 691; \qquad 2221, 2251, 2281, 2311, 2341, 2371.$$

([Mat] 5/57 76).

6.5.17 (Maple)**.** *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 7 (r *oznacza stałą różnicę*).

r	*ciąg*
150	$(7, 157, 307, 457, 607, 757, 907)$
210	$(47, 257, 467, 677, 887, 1097, 1307)$
210	$(179, 389, 599, 809, 1019, 1229, 1439)$
420	$(193, 613, 1033, 1453, 1873, 2293, 2713)$
1050	$(53, 1103, 2153, 3203, 4253, 5303, 6353)$
1260	$(359, 1619, 2879, 4139, 5399, 6659, 7919)$

6.5.18.

(1) *Nie ma żdanego* 7*-wyrazowego ciągu arytmetycznego liczb pierwszych o różnicy* 30. ([Mat] 5/57 75, [S59] 350).

(2) *Jedynym* 7*-wyrazowym ciągiem arytmetycznym liczb pierwszych o różnicy* 150 *jest ciąg* $(7, 157, 307, 457, 607, 757, 907)$. ([S59] 350, [Mat] 2/62 118).

6.5.19 (Maple)**.** *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 8 (r *oznacza stałą różnicę*).

r	*ciąg*
210	$(619, 829, 1039, 1249, 1459, 1669, 1879, 2089)$
210	$(881, 1091, 1301, 1511, 1721, 1931, 2141, 2351)$
630	$(1637, 2267, 2897, 3527, 4157, 4787, 5417, 6047)$
1680	$(1289, 2969, 4649, 6329, 8009, 9689, 11369, 13049)$
2100	$(1847, 3947, 6047, 8147, 10247, 12347, 14447, 16547)$
2310	$(1019, 3329, 5639, 7949, 10259, 12569, 14879, 17189)$

6.5.20 (Maple)**.** *Przykłady ciągów liczb pierwszych tworzących postęp arytmetyczny długości* 9 (r *oznacza stałą różnicę*).

r	*ciąg*
210	$(409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089)$
3150	$(433, 3583, 6733, 9883, 13033, 16183, 19333, 22483, 25633)$
3990	$(1699, 5689, 9679, 13669, 17659, 21649, 25639, 29629, 33619)$
6930	$(17, 6947, 13877, 20807, 27737, 34667, 41597, 48527, 55457)$
7980	$(137, 8117, 16097, 24077, 32057, 40037, 48017, 55997, 63977)$
9240	$(937, 10177, 19417, 28657, 37897, 47137, 56377, 65617, 74857)$

6.5.21. *Dziesięć liczb pierwszych tworzących postęp arytmetyczny:*

$$199,\ 409,\ 619,\ 829,\ 1039,\ 1249,\ 1459,\ 1669,\ 1879,\ 2089.$$

Stała różnica jest równa 210. ([Mat] 3/52 60).

6.5.22. *Dziesięć liczb pierwszych tworzących postęp arytmetyczny:*

$$1847,\ 17807,\ 33767,\ 49727,\ 65687,\ 81647,\ 97607,\ 113567,\ 129527,\ 145487.$$

Stała różnica jest równa 15960. (Maple).

6.5.23. *Jeśli ciąg arytmetyczny* $a_1, \ldots, a_{15}$ *składa się z samych liczb pierwszych, to stała różnica tego ciągu jest większa od* 30 000. ([B-zm] 86).

6.5.24 (J. K. Anderson 2008 [Ande]). *Najmniejsze znane postępy arytmetyczne liczb pierwszych o danej długości n wraz z nazwiskami ich odkrywców i ostatnią liczbą pierwszą. Literą m oznaczono liczby od 0 od $n-1$. Jeśli p jest liczbą pierwszą, to $p\#$ jest iloczynem wszystkich liczb pierwszych mniejszych lub równych p.*

3	$3+2m$	7		
4	$5+6m$	23		
5	$5+6m$	29		
6	$7+30m$	157	1909	*G.Lemaire*
7	$7+150m$	907	1909	*G.Lemaire*
8	$199+210m$	1669	1910	*E.B.Escott*
9	$199+210m$	1879	1910	*E.B.Escott*
10	$199+210m$	2089	1910	*E.B.Escott*
11	$110437+6(11\#)m$	249037	1967	*E.Karst*
12	$110437+6(11\#)m$	262897	1967	*E.Karst*
13	$4943+2(13\#)m$	725663	1963	*V.N.Seredinskij*
14	$31385539+14(13\#)m$	36850999	1983	*P.Pritchard*
15	$115453391+138(13\#)m$	173471351	1983	*P.Pritchard*
16	$53297929+323(13\#)$	198793279	1976	*S.Weintraub*
17	$3430751869+171(17\#)m$	4827507229	1977	*S.Weintraub*
18	$4808316343+1406(17\#)m$	17010526363	1984	*P.Pritchard*
19	$8297644387+431(19\#)m$	83547839407	1984	*P.Pritchard*
20	$214861583621+1943(19\#)m$	572945039351	1987	*J.Young, J.Fry*
21	$5749146449311+2681(19\#)m$	6269243827111	1992	*P.Pritchard*
22	$11410337850553+475180(19\#)m$	108201410428753	1993	*P.Pritchardiinni*
23	$403185216600637+9523(23\#)m$	449924511422857	2006	*M.Frind*
24	$515486946529943+136831(23\#)m$	1217585417914253	2008	*R.Chermoni, J.Wróblewski*
25	$6171054912832631+366384(23\#)m$	8132758706802551	2008	*R.Chermoni, J.Wróblewski*

6.5.25. *Jeśli liczby pierwsze $p_1 < p_2 < \cdots < p_n$ tworzą ciąg arytmetyczny, to $n \leqslant p_1$.*

D. Niech a i b oznaczają odpowiednio wyraz pierwszy i stałą różnicę rozpatrywanego ciągu arytmetycznego. Wtedy $p_i = a + (i-1)b$ dla $i \in \{1, \ldots, n\}$. W szczególności $p_1 = a$. Przypuśćmy, że $p_1 < n$ i rozpatrzmy liczbę p_i dla $i = p_1 + 1$ (oczywiście $i \leqslant n$). Mamy wtedy:

$$p_i = a + (p_1 + 1 - 1)b = p_1 + p_1 b = p_1(1+b).$$

Stąd wynika, że p_i jest większe od p_1 i jest podzielne przez p_1. Jest to sprzeczne z tym, że p_i jest liczbą pierwszą. ⊠

6.5.26 (V.Thébault 1944). *Różnica rosnącego postępu arytmetycznego złożonego z n liczb pierwszych jest podzielna przez iloczyn wszystkich liczb pierwszych mniejszych od n.*
([S59] 348, [S59a] 66).

D. Niech $a,\ a+b,\ a+2b,\ \ldots, a+(n-1)b$ będzie rosnącym ciągiem arytmetycznym składającym się z samych liczb pierwszych. Niech p będzie liczbą pierwszą mniejszą od n i przypuśćmy, że różnica b nie jest podzielna przez p.

Wtedy $p < n \leqslant a$ (na mocy 6.5.25), więc $p \nmid a$. Niech $a = kp + r$, $b = lp + s$, gdzie $k, l \geqslant 0$ oraz $1 \leqslant r, s \leqslant p-1$. Ponieważ p jest liczbą pierwszą, więc istnieje $i \in \{1, 2, \ldots, p-1\}$ takie, że $is \equiv p - r \pmod p$. Mamy wówczas:

$$a + ib = (kp + r) + i(lb + s) \equiv r + (p - r) = p \equiv 0 \pmod p$$

oraz $p < n \leqslant a \leqslant a + ib$. Liczba pierwsza $a + ib$ jest większa od p i jest podzielna przez p. Otrzymaliśmy sprzeczność. ⊠

6.5.27. *Załóżmy, że liczby pierwsze $p_1 < p_2 < \cdots < p_n$ tworzą ciąg arytmetyczny o różnicy b. Jeśli b nie jest podzielne przez liczbę pierwszą q, to $n \leqslant q$.*
([Mat] 5/1996 s.267, [Gr08], wynika to natychmiast z 6.5.26).

6.5.28. *Niech $n = p$ będzie liczbą pierwszą i załóżmy, że liczby pierwsze $p_1 < p_2 < \cdots < p_n$ tworzą ciąg arytmetyczny o różnicy b. Jeśli $p \nmid b$, to $p_1 = p$.* ([Mat] 5/1996 s.266).

D. Powtarzamy dowód faktu 6.5.26. Niech $a,\ a+b,\ a+2b,\ \ldots, a+(n-1)b$ będzie danym ciągiem arytmetycznym liczb pierwszych. Załóżmy, że $p \nmid b$ i przypuśćmy, że $p_1 \neq p$. Ale $p_1 = a$, więc $p \nmid a$. Niech $a = kp + r$, $b = lp + s$, gdzie $k, l \geqslant 0$ oraz $1 \leqslant r, s \leqslant p-1$. Ponieważ p jest liczbą pierwszą, więc istnieje $i \in \{1, 2, \ldots, p-1\}$ takie, że $is \equiv p - r \pmod p$. Mamy wówczas:

$$a + ib = (kp + r) + i(lb + s) \equiv r + (p - r) = p \equiv 0 \pmod p$$

oraz $p = n \leqslant a < a + ib$ (na mocy 6.5.25). Liczba pierwsza $a + ib$ jest większa od p i jest podzielna przez p. Otrzymaliśmy sprzeczność. ⊠

6.5.29. *Dla każdej liczby naturalnej m istnieje nieskończenie wiele liczb naturalnych a takich, że każda z liczb $a+1,\ 2a+1,\ 3a+1, \ldots,\ ma+1$ jest złożona.* ([S59] 328).

★ W. Bednarek, *Arytmetyczne ciągi liczb pierwszych*, [Mat] 5/1996 266-270.
R. K. Guy, *Arithmetic progressions of primes*, [Gy04] 25-28.
R. K. Guy, *Consecutive primes in arithmetic progressions*, [Gy04] 28-30.
W. Sierpiński, *Arithmetical progressions whose terms are prime numbers*, [S88] 126-128.
J. Wróblewski, *How to search for* 26 *primes in arithmetic progression?*, [Wmm], 227-232.

6.6 Uogólnione postępy arytmetyczne liczb pierwszych

Niech d będzie liczbą naturalną i niech $N_1, \ldots, N_d$ będą liczbami naturalnymi większymi od 1. *Uogólnionym ciągiem arytmetycznym*, wymiaru d i objętości $(N_1, \ldots, N_d)$, nazywamy każdy zbiór postaci

$$\Big\{a + i_1b_1 + i_2b_2 + \cdots + i_db_d;\ i_1 \in \{0, 1, \ldots, N_1 - 1\}, \ldots, i_d \in \{0, 1, \ldots, N_d - 1\}\Big\},$$

gdzie $a, b_1, b_2, \ldots, b_d$ są liczbami naturalnymi ([Gr08]). Powyższy zbiór oznaczać będziemy przez $[a, (b_1, b_2, \ldots, b_d)]$.

Każdy skończony ciąg arytmetyczny liczb naturalnych, o różnicy większej od 1, jest uogólnionym ciągiem arytmetycznym wymiaru 1. Zbiór

$$[3, (8, 2)] = \Big\{3 + 8i + 2j;\ i \in \{0, 1\}, j \in \{0, 1\}\Big\}$$

jest ugólnionym ciągiem arytmetycznym wymiaru 2 i objętości $(2, 2)$. Jest to zbiór liczbowy $\{3, 5, 11, 13\}$. Każdy element tego zbioru jest liczbą pierwszą. Podobną własność ma zbiór

$$[7, (24, 6)] = \Big\{7 + 24i + 6j;\ i \in \{0, 1\}, j \in \{0, 1, 2\}\Big\} = \Big\{7, 13, 19, 31, 37, 43\Big\},$$

będący uogólnionym ciągiem arytmetycznym wymiaru 2 i objętości $(2, 3)$. Każdy element jest liczbą pierwszą.

Każdy uogólniony ciąg arytmetyczny objętości $(N_1, \ldots, N_d)$ ma co najwyżej $N_1N_2 \cdots N_d$ elementów. Może tych elemntów być mniej niż $N_1 \cdots N_d$. Dla przykładu uogólniony ciąg $[3, (2, 2)]$, wymiaru 2 i objętości $(2, 2)$, ma tylko trzy elementy: 3, 5 i 7.

Niech $[a, (b_1, \ldots, b_d)]$ będzie uogólnionym ciągiem arytmetycznym wymiaru d i obętości $(N_1, \ldots, N_d)$. Mówić będziemy, że ciąg ten jest *specjalny*, jeśli ma dokładnie $N_1 N_2 \cdots N_d$ elementów oraz każdy jego element jest liczbą pierwszą.

6.6.1 ([Gr08]). *Przykłady specjalnych uogólnionych ciągów arytmetycznych wymiaru* 2. *W każdym przypadku podano również objętość i największą liczbę pierwszą.*

$(2,2)$	$[3,(8,2)]$	13
$(2,3)$	$[7,(24,6)]$	43
$(2,4)$	$[5,(36,6)]$	59
$(2,5)$	$[11,(96,30)]$	227
$(2,6)$	$[11,(42,60)]$	353
$(2,7)$	$[47,(132,210)]$	1439
$(2,8)$	$[199,(3300,210)]$	4969
$(2,9)$	$[199,(3300,210)]$	5179

$(3,3)$	$[5,(12,42)]$	113
$(3,3)$	$[29,(12,30)]$	113
$(4,3)$	$[11,(90,36)]$	353
$(4,4)$	$[503,(360,1218)]$	5237

6.6.2 (Maple). *Przykłady specjalnych uogólnionych ciągów wymiaru* 2 *i objętości* $(2,2)$*:*

$$[3,(2,8)],\ [3,(2,14)],\ [5,(2,6)],\ [7,(4,6)],\ [11,(2,6)],\ [13,(4,6)].$$

6.6.3 (Maple). *Przykłady specjalnych uogólnionych ciągów wymiaru* 2 *i objętości* $(2,3)$*:*

$$[5,(2,6)],\ [7,(4,6)],\ [11,(2,30)],\ [13,(6,24)],\ [17,(2,12)],\ [19,(4,24)].$$

6.6.4 (Maple). *Przykłady specjalnych uogólnionych ciągów wymiaru* 2 *i objętości* $(2,4)$*:*

$$[5,(2,12)],\ [7,(4,30)],\ [11,(2,30)],\ [13,(10,30)],\ [17,(30,12)],\ [19,(10,54)].$$

6.6.5 (Maple). *Przykłady specjalnych uogólnionych ciągów wymiaru* 2 *i objętości* $(2,5)$*:*

$$[7,(4,30)],\ [11,(26,30)],\ [13,(4,150)],\ [17,(56,150)],\ [23,(24,210)],\ [29,(78,120)].$$

6.6.6 (Maple). *Przykłady specjalnych uogólnionych ciągów arytmetycznych wymiaru* 2 *o danej objętości.*

$(3,3)$	$[7,(30,36)]$
$(3,3)$	$[11,(18,60)]$
$(3,3)$	$[13,(30,84)]$

$(3,4)$	$[11,(90,126)]$
$(3,4)$	$[13,(168,30)]$
$(3,4)$	$[19,(24,420)]$

$(3,5)$	$[19,(24,420)]$
$(3,5)$	$[23,(24,210)]$
$(3,5)$	$[97,(1890,780)]$

6.6.7. *Niech* $[a, (b_1, b_2, \ldots, b_d)]$ *będzie uogólnionym ciągiem arytmetycznym wymiaru* d *i objętości* $(N_1, \ldots, N_d)$*, składającym się z samych liczb pierwszych. Wówczas każda liczba* b_i*, dla* $i = 1, 2, \ldots, d$*, jest podzielna przez wszystkie liczby pierwsze mniejsze od* N_i*.* (Wynika to z 6.5.26).

Korzystając z twierdzenia Greena i Tao 6.5.8, można udowodnić:

6.6.8 (A. Granville 2008). *Dla każdej liczby naturalnej* d *i dowolnych liczb naturalnych* N_1*, ...,* $N_d \geqslant 2$*, istnieje nieskończenie wiele specjalnych uogólnionych ciągów arytmetycznych, wymiaru* d *i objętości* $(N_1, \ldots, N_d)$*.* ([Gr08]).

D. ([Gr08]). Niech $q = \max\{N_1, \ldots, N_d\}$, $n = q^d$. Niech $A = \{a + jr;\ j = 0, 1, \ldots, n-1\}$ będzie n-wyrazowym ciągiem arytmetycznym liczb pierwszych. Taki ciąg istnieje na mocy twierdzenia 6.5.8.

Przyjmijmy: $b_1 = q^0 r,\ b_2 = q^1 r,\ \ldots,\ b_d = q^{d-1} r$ i rozpatrzmy zbiór

$$B = \Big\{a + i_1 b_1 + i_2 b_2 + \cdots + i_d b_d;\ i_1 \in \{0, 1, \ldots, N_1 - 1\}, \ldots, i_d \in \{0, 1, \ldots, N_d - 1\}\Big\}.$$

Jest to uogólniony ciąg arytmetyczny wymiaru d i objętości $(N_1, \ldots, N_d)$.

Pokażemy, że $B \subseteq A$. Niech $x \in B$. Wtedy

$$x = a + i_1 b_1 + \cdots + i_d b_d = a + \left(i_1 q^0 + i_2 q^1 + \cdots + i_d q^{d-1}\right) r = a + jr,$$

gdzie $j = i_1 q^0 + i_2 q^1 + \cdots + i_d q^{d-1} \leqslant (q-1)\left(q^0 + q^1 + \cdots + q^{d-1}\right) = q^d - 1 = n - 1$. Zatem $x = a + jr \in A$. Każdy więc element zbioru B jest liczbą pierwszą. Z jednoznaczności zapisu liczb przy danej podstawie numeracji wynika, że wszystkie rozpatrywane liczby pierwsze są parami różne. Zbiór B spełnia zatem żądane warunki. Z tej konstrukcji wynika oczywiście, że takich uogólnionych ciągów arytmetycznych istnieje nieskończenie wiele. ⊠

ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

6.7 Twierdzenie Baloga i jego uogólnienia

ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

W 2005 roku B.Green i T.Tao udowodnili, że dla każdej liczby naturalnej n istnieje nieskończenie wiele n-wyrazowych postępów arytmetycznych utworzonych z parami różnych liczb pierwszych (patrz twierdzenie 6.5.8). Z twierdzenia tego wynika, na przykład, że dla każdej liczby naturalnej d i dowolnych liczb naturalnych $N_1, \ldots, N_d \geqslant 2$, istnieje nieskończenie wiele uogólnionych ciągów arytmetycznych, wymiaru d i objętości $(N_1, \ldots, N_d)$, składających się z samych liczb pierwszych (patrz 6.6.8). Teraz przedstawimy pewne inne zastosowania twierdzenia Greena i Tao.

Średnia arytmetyczna liczb pierwszych 3 i 7 jest równa 5, jest więc liczbą pierwszą (i to różną od 3 i 7). Zbiór $\{3, 7, 19\}$ składa się z trzech liczb pierwszych. Mamy tu trzy średnie arytmetyczne: $\frac{3+7}{2} = 5$, $\frac{3+19}{2} = 11$ i $\frac{7+19}{2} = 13$. Wszystkie te średnie są liczbami pierwszymi i przy tym różnymi od 3, 7 i 19.

Podobną własność ma zbiór $\{3, 11, 23, 71\}$, składający się z czterech liczb pierwszych. Wszystkie średnie arytmetyczne postaci $\frac{a+b}{2}$ są liczbami pierwszymi:

$$\tfrac{3+11}{2} = 7,\ \tfrac{3+23}{2} = 13,\ \tfrac{3+71}{2} = 37,\ \tfrac{11+23}{2} = 17,\ \tfrac{11+71}{2} = 41,\ \tfrac{23+71}{2} = 47.$$

Ponadto, wszystkie występujące tu liczby pierwsze są parami różne.

6.7.1 ([Gr08])**.** *Przykłady n-elementowych ciągów liczb pierwszych posiadających powyżej rozważaną własność (dla $n = 2, 3, \ldots, 8$).*

2	$3, 7$
3	$3, 7, 19$
4	$3, 11, 23, 71$
5	$3, 11, 23, 71, 191$
6	$3, 11, 23, 71, 191, 443$
7	$5, 17, 41, 101, 257, 521, 881$
8	$257, 269, 509, 857, 1697, 2309, 2477, 2609$

W [Gr08] znajdziemy również takie przykłady dla $n = 9, 10, 11$ i 12. Są to "najmniejsze" tego rodzaju przykłady. A. Balog ([Balo]) udowodnił w 1990 roku, że takie przykłady można skonstruować dla każdej liczby naturalnej n.

6.7.2 (A.Balog 1990)**.** *Dla każdej liczby naturalnej $n \geqslant 2$ istnieją liczby pierwsze $p_1 < p_2 < \cdots < p_n$ takie, że każda średnia arytmetyczna postaci $\frac{p_i+p_j}{2}$ też jest liczbą pierwszą. Ponadto, zbiorów $\{p_1, \ldots, p_n\}$ o takiej własności jest nieskończenie wiele.* ([Balo])*.*

D. ([Gr08]). Niech $A = \{a + jd;\ j = 0, 1, \ldots, 2n-1\}$ będzie $2n$-wyrazowym ciągiem arytmetycznym liczb pierwszych. Taki ciąg istnieje na mocy twierdzenia 6.5.8. Rozpatrzmy podzbiór

$$B = \{a + 2jd;\ j = 0, 1, \ldots, n-1\}.$$

Jest to n-elementowy zbiór składający się z samych liczb pierwszych. Zbiór ten ma żądaną własność. Jeśli $p_i = a + 2id,\ \ p_j = a + 2jd$ są elementami zbioru B, to

$$\tfrac{p_i+p_j}{2} = \tfrac{2a+2(i+j)d}{2} = a + (i+j)d \in A$$

i stąd wynika, że $\frac{p_i+p_j}{2}$ jest liczbą pierwszą. Ponieważ zbiorów postaci A istnieje (na mocy twierdzenia 6.5.8) nieskończenie wiele, więc rozważanych zbiorów istnieje również nieskończenie wiele. ☒

6.7.3 (A.Balog 1990)**.** *Dla każdej liczby naturalnej $n \geqslant 2$ istnieją liczby pierwsze $p_1 < p_2 < \cdots < p_n$ takie, że każda średnia arytmetyczna postaci $\frac{p_i+p_j}{2}$ też jest liczbą pierwszą oraz wszystkie liczby pierwsze postaci $\frac{p_i+p_j}{2}$, gdzie $i \leqslant j$, są parami różne. Ponadto, zbiorów $\{p_1, \ldots, p_n\}$ o takiej własności jest nieskończenie wiele.* ([Balo]).

D. ([Gr08]). Niech $A = \{a + jd;\ j = 0, 1, \ldots, 2^n\}$ będzie (2^n+1)-wyrazowym ciągiem arytmetycznym liczb pierwszych. Taki ciąg istnieje na mocy twierdzenia 6.5.8. Rozpatrzmy podzbiór

$$B = \Big\{a + 2^j d;\ j = 1, 2, \ldots, n\Big\}.$$

Jest to n-elementowy zbiór składający się z samych liczb pierwszych. Zbiór ten ma żądaną własność. Jeśli $p_i = a + 2^i d,\ \ p_j = a + 2^j d$ są elementami zbioru B, to

$$\tfrac{p_i+p_j}{2} = \tfrac{2a+(2^i+2^j)d}{2} = a + \left(2^{i-1} + 2^{j-1}\right) d \in A$$

i stąd wynika, że $\frac{p_i+p_j}{2}$ jest liczbą pierwszą. Z jednoznaczności przedstawienia liczb naturalnych w systemie numeracji o podstawie 2 wynika, że wszystkie pojawiające się tu liczby pierwsze są parami różne. Ponieważ zbiorów postaci A istnieje (na mocy twierdzenia 6.5.8) nieskończenie wiele, więc rozważanych zbiorów istnieje również nieskończenie wiele. ☒

Powyższe twierdzenia Baloga można uogólnić w następujący sposób.

6.7.4 (A.Granville 2008)**.** *Dla każdej liczby naturalnej $n \geqslant 2$ istnieje n-elementowy zbiór liczb pierwszych taki, że średnia arytmetyczna dowolnego jego niepustego podzbioru też jest liczbą pierwszą. Ponadto, n-elementowych zbiorów o takiej własności jest nieskończenie wiele.* ([Gr08]).

D. ([Gr08]). Niech $k = n \cdot n!$ i niech $A = \{a + jd;\ j = 0, 1, \ldots, k-1\}$ będzie k-wyrazowym ciągiem arytmetycznym liczb pierwszych. Taki ciąg istnieje na mocy twierdzenia 6.5.8. Rozpatrzmy podzbiór

$$B = \{a + j \cdot n! \cdot d;\ j = 0, 1, \ldots, n-1\}.$$

Jest to n-elementowy zbiór składający się z samych liczb pierwszych. Zbiór ten ma żądaną własność. Niech I będzie dowolnym niepustym podzbiorem zbioru B. Średnia arytmetyczna tego podzbioru jest równa:

$$\frac{1}{|I|}\sum_{i\in I}(a + i \cdot n! \cdot d) = a + d\left(\sum_{i\in I} i\right)\frac{n!}{|I|}$$

i jest oczywiste, że ona należy do zbioru A, czyli jest liczbą pierwszą. Ponieważ zbiorów postaci A istnieje (na mocy twierdzenia 6.5.8) nieskończenie wiele, więc rozważanych zbiorów istnieje również nieskończenie wiele. ☒

6.7.5 (A.Granville 2008)**.** *Dla każdej liczby naturalnej $n \geqslant 2$ istnieje n-elementowy zbiór liczb pierwszych taki, że średnia arytmetyczna dowolnego jego niepustego podzbioru też jest liczbą pierwszą i wszystkie te liczby pierwsze są parami różne. Ponadto, n-elementowych zbiorów o takiej własności jest nieskończenie wiele.* ([Gr08]).

D. ([Gr08]). Niech $k = 2^n n! + 1$ i niech $A = \{a + jd;\ j = 0, 1, \ldots, k-1\}$ będzie k-wyrazowym ciągiem arytmetycznym liczb pierwszych. Taki ciąg istnieje na mocy twierdzenia 6.5.8. Rozpatrzmy podzbiór

$$B = \{a + \left(2^j n!\right) d;\ j = 1, 2, \ldots, n\}.$$

Jest to n-elementowy zbiór składający się z samych liczb pierwszych i łatwo sprawdzić, że ten zbiór posiada rozważaną własność. Ponieważ zbiorów postaci A istnieje (na mocy twierdzenia 6.5.8) nieskończenie wiele, więc zbiorów B również jest nieskończenie wiele. ⊠

6.7.6 ([Gr08])**.** *Przykłady n-elementowych ciągów liczb pierwszych posiadających powyżej rozważaną własność (dla $n = 2, 3, 4, 5$).*

2	3, 7
3	7, 19, 67
4	5, 17, 89, 1277
5	209173, 332573, 536773, 1217893, 2484733

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

6.8 Nieskończone postępy arytmetyczne i liczby pierwsze

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

6.8.1. *W każdym ciągu arytmetycznym o wyrazach naturalnych i różnicy naturalnej istnieje nieskończenie wiele liczb złożonych.*

D. Niech $(a + bn)$, $a, b \in \mathbb{N}$ będzie ciągiem arytmetycznym. Jeśli $(a, b) > 1$, to nie ma czego dowodzić. Jeśli $a > 1$, to przyjmując $n = ka$ $(k = 1, 2, \ldots)$ mamy nieskończenie wiele liczb złożonych. Jeśli $a = 1$, to dla $n_k = 4bk^2 + 4k$ mamy: $a + bn_k = (2bk + 1)^2$. ⊠

6.8.2. *W każdym nieskończonym postępie arytmetycznym o wyrazach całkowitych istnieje nieskończenie wiele wyrazów posiadających jednakowe dzielniki pierwsze.* ([S64] 60, [Kw] 6/73 46).

6.8.3. *W każdym postępie arytmetycznym postaci $(ak+b)$, gdzie $(a, b) = 1$, istnieje nieskończenie wiele parami względnie pierwszych wyrazów.* ([S64] 59).

6.8.4. *Dla każdego $n \in \mathbb{N}$ istnieje n liczb złożonych tworzących ciąg arytmetyczny, z których każde dwie są względnie pierwsze.* ([Mon] 76(2)(1969) E2062).

6.8.5. *Niech $(a, b) = 1$. Dla każdej liczby naturalnej m w postępie arytmetycznym $(ak + b)$ istnieje nieskończenie wiele wyrazów względnie pierwszych z m.* ([S64] 54).

D. ([S64]). Możemy oczywiście założyć, że $m \geqslant 2$. Niech u, v, w będą liczbami naturalnymi zdefiniowanymi następująco:

$u =$ iloczyn wszystkich różnych dzielników pierwszych liczby m, które są dzielnikami liczby a; jeśli takich nie ma, to niech $u = 1$.

$v =$ iloczyn wszystkich różnych dzielników pierwszych liczby m, które są dzielnikami liczby b; jeśli takich nie ma, to niech $v = 1$.

$w =$ iloczyn wszystkich różnych dzielników pierwszych liczby m, które nie są dzielnikami ani liczby a ani liczby b; jeśli takich nie ma, to niech $w = 1$.

Jest jasne, że $(u,w)=1$, $(v,w)=1$ oraz $(u,v)=1$. Stąd wynika, że liczba $auw+b$ jest względnie pierwsza z m. Każda zatem liczba postaci $a(uw+km)+b$, gdzie $k\in\mathbb{N}$, jest względnie pierwsza z m. Liczb takich jest nieskończenie wiele. ⊠

6.8.6. *Nie istnieje nieskończony rosnący ciąg arytmetyczny liczb naturalnych taki, że zbiór dzielników pierwszych wyrazów tego ciągu jest skończony.* ([Mat] 2/2000 z.1471).

D. Przypuśćmy, że taki ciąg istnieje. Niech a będzie wyrazem pierwszym tego ciągu, a r jego różnicą. Niech $\{p_1,\ldots,p_s\}$ nędzie zbiorem wszystkich liczb pierwszych dzielących jego wyrazy. Rozpatrzmy wyraz o numerze $n=ap_1p_2\ldots p_s+1$. Jest on równy $a(1+rp_1p_2\cdots p_s)$. Liczba $1+rp_1p_2\cdots p_s$ jest większa od 1, dzieli się więc przez jakąś liczbę pierwszą q i jest oczywiste, że q nie należy do zbioru $\{p_1,\ldots,p_s\}$. Z drugiej jednak strony q należy do tego zbioru, gdyż dzieli wspomniany powyżej wyraz. Otrzmaliśmy sprzeczność. ⊠

6.8.7. *W ciągu arytmetycznym $(30k+7)$ żaden wyraz nie jest sumą ani różnicą dwóch liczb pierwszych.* ([S64] 65).

6.8.8. *Niech $a,b,n\in\mathbb{N}$, $(a,b)=1$. Niech $\mathbb{D}$ będzie nieskończonym zbiorem pewnych liczb postaci $ak+b$, gdzie $k\in\mathbb{N}$. Wówczas istnieje liczba postaci $ak+b$, która jest iloczynem co najmniej n parami różnych elementów zbioru $\mathbb{D}$.* ([S59] 192).

D. Niech $s=m\varphi(a)+1$. Niech $q_1,\ldots,q_s$ będą parami różnymi elementami zbioru $\mathbb{D}$. Wtedy $q_i\equiv b\,(\mathrm{mod}\ a)$ dla $i=1,2,\ldots,s$, skąd

$$q_1\cdots q_s\equiv b^s\equiv b^{m\varphi(a)}b\equiv\equiv b\pmod a.$$

Zatem $q_1\cdots q_s$ jest liczbą postaci $ak+b$ i oczywiście $s>m$. ⊠

6.8.9. *Niech $a,b\in\mathbb{N}$, $(a,b)=1$. W ciągu arytmetycznym $(an+b)$ istnieje nieskończenie wiele liczb potęgowych.* ([Mon] 71(6)(1964) E1710).

6.8.10. *Niech $a,b,n\in\mathbb{N}$, $(a,b)=1$. Istnieje nieskończenie wiele liczb postaci $ak+b$, gdzie $k\in\mathbb{N}$, będących iloczynami n parami różnych liczb pierwszych.* ([S59] 192, [S64] 61).

D. Niech m będzie dowolną liczbą naturalną. Z twierdzenia Dirichleta o liczbach pierwszych w postępie arytmetycznym wynika, że istnieje liczba pierwsza $p_1>m$ postaci $ak+b$. Z tego twierdzenia wynika również, że istnieją liczby pierwsze $p_2,p_3,\ldots,p_n$ postaci $ak+1$ takie, że $p_1<p_2<\cdots<p_n$. Mamy zatem p_1ba oraz $p_i\equiv 1\,(\mathrm{mod}\ a)$ dla $i=2,3,\ldots,n$. Zatem $p_1p_2\cdots p_n\equiv b\,(\mathrm{mod}\ a)$, czyli $p_1p_2\cdots p_n$ jest liczbą postaci $ak+b$ większą od m (bo $p_1>m$). ⊠

★ P. Morton, *Musings on the prime divisors of arithmetic sequences*, [Mon] 97(4)(1990) 323-328.

Literatura

[Ama] The AMATYC Review.

[Ande] J. K. Anderson, *Primes in arithmetic progression records*, `http://hjem.get2net.dk/jka/math/aprecords.htm`.

[AnnM] Annals of Mathematics, (Ann. of Math.).

[B-ew] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society, Monographs and Advanced Texts 21, John Wiley and Sons, INC, 1998.

[B-rs] J. Browkin, J. Rempała, S. Straszewicz, *25 lat Olimpiady Matematycznej*, WSiP, Warszawa, 1975.

[B-zm] V. I. Bernik, I. K. Żuk, O. W. Melnikow, *Zbiór Zadań Olimpijskich z Matematyki* (po rosyjsku), Narodnaja Aswieta, Minsk, 1980.

[Balk] Balkan Mathematical Olympiad.

[Balo] A. Balog, *The prime k-tuples conjecture on average*, Analytic Number Theory, B.C. Berndt et al., des., Birkhäuser, Boston, 1990, 165-204.

[Br83] J. Browkin, *Zbiór Zadań z Olimpiad Matematycznych*, tom 6, 26-30, 74/75 - 78/79, WSiP, Warszawa, 1983.

[Fila] M. Filaseta, *The Theory of Irreducible Polynomials*, Preprint, 2000. `http://www.math.sc.edu/~filaseta`.

[G-ns] A. I. Gałoczkin, Ju. W. Nesterenko, A. B. Szydłowski, *Wstęp do Teorii Liczb* (po rosyjsku), Moskwa, 1984.

[G-T] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. Math. (to appear); also available at `http://xxx.arxiv.org/math.NT/0404188`.

[Gr08] A. Granville, *Prime number patterns*, The American Mathematical Monthly, 115(4)(2008), 279-296.

[Gy04] R. K. Guy, *Unsolved Problems in Number Theory*, Third edition, Springer-Verlag, New York, 2004.

[IMO] Międzynarodowa Olimpiada Matematyczna.

[IrR] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer - Verlag New York Inc., New York, 1982.

[Kw] Kwant, popularne czasopismo rosyjskie.

[Land] E. Landau, *Elementary Number Theory*, AMS Chelsea Publishing 1999, przedruk z 1927 r.

[Mat] Matematyka, polskie czasopismo dla nauczycieli.

[Miss] Missouri Journal of Mathematical Sciences.

[MM] Mathematics Magazine, popularne czasopismo matematyczne.

[Mon] The American Mathematical Monthly, Mathematical Association of America.

[Nagl] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1964.

[Nar03] W. Narkiewicz, *Teoria Liczb*, PWN, Wydanie trzecie, Warszawa, 2003.

[Nar77] W. Narkiewicz, *Teoria liczb*, PWN, Warszawa, 1977.

[OM] Olimpiada Matematyczna.

[OMs] Sprawozdanie Komtetu Głównego Polskiej Olimpiady Matematycznej.

[Pmgr] Praca magisterska, Uniwersytet Mikołaja Kopernika w Toruniu, Wydział Matematyki i Informatyki.

[Po82] M. M. Postnikov, *Wstęp do teorii liczb algebraicznych*, (po rosyjsku), Nauka, Moskwa, 1982.

[S50] W. Sierpiński, *Teoria Liczb*, Warszawa - Wrocław, 1950.

[S59] W. Sierpiński, *Teoria Liczb* II, PWN, Warszawa, 1959.

[S59a] W. Sierpiński, *O Stu Prostych, ale Trudnych Zagadnieniach Arytmetyki. Z Pogranicza Geometrii i Arytmetyki*, Biblioteczka Matematyczna 6, PZWS, Warszawa, 1959.

[S64] W. Sierpiński, *200 Zadań z Elementarnej Teorii Liczb*, Biblioteczka Matematyczna 17, PZWS, Warszawa, 1964.

[S88] W. Sierpiński, *Elementary Theory of Numbers*, Editor: A. Schinzel, North-Holland Mathematical Library, Vol. 31, 1988.

[Str] S. Straszewicz, *Zadania z Olimpiad Matematycznych*, tom I, 1-5, 49/50 - 53/54, PZWS, Warszawa, 1960.

[Str67] S. Straszewicz, *Zadania z Olimpiad Matematycznych*, tom III, 11-15, 59/60 - 63/64, PZWS, Warszawa, 1967.

[Trost] E. Trost, *Primzahlen*, Verlag Birkhauser, Basel - Stuttgard. Tłumaczenie rosyjskie, Moskwa 1959.

[TT] Tournament of the Towns.

[WaJ] N. B. Wasilev, A. A. Jegorow, *Zadania Olimpiad Matematycznych Związku Radzieckiego* (po rosyjsku), 1961-1987, Moskwa, Nauka, 1988.

[Wm] Wiadomości Matematyczne, Roczniki Polskiego Towarzystwa Matematycznego, 1956-2012.

[Wmm] XI Międzynarodowe Warsztaty dla Młodych Matematyków, *Teoria Liczb*, Uniwersytet Jagielloński, Kraków 2009.